INTELLIGENCE INFO

ISSN 2821 - 8159, ISSN – L 2821 – 8159, Volumul 2, Numărul 4, Decembrie 2023

Evoluția inteligenței artificiale în domeniul securității naționale

Nicolae Sfetcu

Sfetcu, Nicolae (2023), Evoluția inteligenței artificiale în domeniul securității naționale, *Intelligence Info*, **2**:4, 3-11, DOI: 10.58679/II35704, https://www.intelligenceinfo.org/evolutia-inteligentei-artificiale-in-domeniul-securitatii-nationale/

Publicat online: 10.11.2023

Evoluția inteligenței artificiale în domeniul securității naționale

Ing. fiz. Nicolae Sfetcu, MPhil[1]
nicolae@sfetcu.com

The evolution of artificial intelligence in the field of national security

Abstract

Artificial intelligence is a rapidly growing technology field that is capturing the attention of defense, policy makers, and international competitors alike. Artificial intelligence is increasingly playing a significant role in intelligence analysis, which is the process of collecting, evaluating and interpreting information to produce actionable intelligence, and national security in general. Intelligence services around the world are increasingly using artificial intelligence and machine learning techniques to improve their capabilities in various aspects of their work. Artificial intelligence can significantly improve the collection, analysis and targeted dissemination of intelligence.

Keywords: intelligence agencies, artificial intelligence, military, defense, national security, intelligence

Rezumat

Inteligența artificială este un domeniu tehnologic în creștere rapidă, care captează atenția în domeniul apărării, factorilor de decizie politică și concurenților internaționali deopotrivă. Inteligența artificială joacă din ce în ce mai mult un rol semnificativ în analiza inteligenței, care este procesul de colectare, evaluare și interpretare a informațiilor pentru a produce inteligență acționabilă, și securitatea națională în general. Serviciile de informații din întreaga lume folosesc din ce în ce mai mult inteligența artificială și tehnicile de învățare automată pentru a-și îmbunătăți capacitățile în diferite aspecte ale activității lor.

[1] Academia Română – Comitetul Român de Istoria și Filosofie Științei și Tehnicii (CRIFST), Divizia de Istoria Științei (DIS)

Inteligența artificială poate îmbunătăți semnificativ colectarea, analiza și diseminarea țintită a activității de intelligence.

Cuvinte cheie: servicii de informații, inteligența artificială, armata, apărare, securitatea națională, intelligence

INTELLIGENCE INFO, Volumul 2, Numărul 4, Decembrie 2023, pp. 3-11
ISSN 2821 - 8159, ISSN – L 2821 – 8159, DOI: 10.58679/II35704
URL: https://www.intelligenceinfo.org/evolutia-inteligentei-artificiale-in-domeniul-securitatii-nationale/

Introducere

Inteligența artificială (IA) este un domeniu tehnologic în creștere rapidă, care captează atenția în domeniul apărării, factorilor de decizie politică și concurenților internaționali deopotrivă. Inteligența artificială joacă din ce în ce mai mult un rol semnificativ în analiza inteligenței, care este procesul de colectare, evaluare și interpretare a informațiilor pentru a produce inteligență acționabilă, și securitatea națională în general. Serviciile de informații din întreaga lume folosesc din ce în ce mai mult inteligența artificială și tehnicile de învățare automată pentru a-și îmbunătăți capacitățile în diferite aspecte ale activității lor. IA poate îmbunătăți semnificativ colectarea, analiza și diseminarea țintită a activității de intelligence.

Inteligența artificială va avea implicații imense pentru securitatea națională și internațională, iar potențialele aplicații ale inteligenței artificiale pentru apărare și intelligence sunt o prioritate majoră. Marile națiuni investesc în prezent sume imense în aplicații militare ale inteligenței artificiale, obținând un avantaj competitiv net față de țările care neglijează această oportunitate.

Serviciile de informații sunt însărcinate cu colectarea, analizarea și interpretarea informațiilor pentru a proteja securitatea națională. În epoca modernă, volumul și

complexitatea datelor au crescut exponențial, necesitând încorporarea unor tehnologii avansate, cum ar fi inteligența artificială, pentru a le îmbunătăți capacitățile. IA are potențialul de a revoluționa operațiunile de informații, îmbunătățind viteza, acuratețea și eficiența procesării și analizei datelor. Serviciile de informații au început să identifice inteligența artificială ca o tehnologie cheie pentru menținerea avantajului față de adversari și protejarea împotriva amenințărilor.

Analiza intelligence este o componentă vitală a securității naționale, servind drept fundație pe care se iau decizii informate pentru a proteja interesele unei națiuni. Complexitatea amenințărilor moderne de securitate necesită instrumente și metodologii avansate, iar una dintre cele mai promițătoare evoluții în acest sens este integrarea inteligenței artificiale în procesul de analiză a intelligence.

Evoluția inteligenței artificiale

Rolul IA în analiza intelligence a evoluat semnificativ de-a lungul anilor. Inițial, inteligența artificială a fost folosită în principal pentru gestionarea și procesarea datelor, reducând sarcina supraîncărcării de informații asupra analiștilor. Odată cu progresele în învățarea automată, procesarea limbajului natural și învățarea profundă, IA poate îndeplini acum sarcini analitice mai complexe, oferind un nivel complementar de perspectivă analiștilor umani.

Serviciile de informații au folosit inteligența artificială încă de la începutul războiului rece. Traducerea automată a documentelor în limbi străine a pus bazele tehnicilor moderne de procesare a limbajului natural (NLP). De la sfârșitul războiului rece, analiza imaginilor a ajutat la identificarea posibililor teroriști, analizând informațiile și făcând predicții[2]. Astfel, în SUA s-a creat Sistemul de Supraveghere a Sunetului (SOSUS), o rețea de senzori acustici subacvatici pentru a acționa ca posturi de ascultare subacvatice pentru instalațiile supraterane[3].

La finele anilor 1990, Departamentul Apărării SUA a dezvoltat planuri pentru un război „centrat pe rețea” prin integrarea inteligenței artificiale[4]. Exemple de proiecte sunt

[2] (Townley 2023)
[3] (Lakhwani et al. 2020)
[4] (Day 2016)

Nett Warrior (fost Ground Soldier System sau Mounted Soldier System)[5] și Force XXI Battle Command Brigade[6].

În secolul XXI, organizațiile din domeniul securității naționale folosesc inteligența artificială pentru a le ajuta să găsească, conform lui Dan Coats în 2017, „modalități inovatoare de a exploata și de a stabili relevanța și de a asigura veridicitatea informațiilor”[7].

În jurul anului 2010 a avut loc o explozie a interesului pentru IA, datorită convergenței a trei evoluții favorabile[8]: (1) disponibilitatea surselor de megadate („big data”), (2) îmbunătățiri ale abordărilor de învățare automată, și (3) creștea puterii de procesare[9]. Astfel s-a dezvoltat forma slabă a IA, cu algoritmi pentru probleme specifice, precum jocul, recunoașterea imaginilor și navigarea. Progresele rapide în IA au declanșat un val de investiții. Investițiile neclasificate ale DoD (SUA) în IA au crescut de la puțin peste 600 de milioane de dolari în exercițiul financiar 2016 la 2,5 miliarde de dolari în exercițiul financiar 2021, cu peste 600 de proiecte active de IA[10][11].

În 2011, Autoritatea Națională de Securitate Cehă (NSA) a fost numită ca autoritate națională pentru agenda cibernetică, cu o strategie specială pentru integrarea inteligenței artificiale și apărarea securității naționale din această perspectivă[12].

La nivelul Uniunii Europene, adoptarea Strategiei de securitate cibernetică în 2013 de către Comisia Europeană[13] a impulsionat eforturile de implementare a inteligenței artificiale. UE finanțează diverse programe și instituții în acest sens, precum Competence Research Innovation (CONCORDIA), care reunește 14 state membre[14] și Cybersecurity for Europe (CSE)[15], care reunește 43 de parteneri care implică 20 de state membre. Rețeaua Europeană a Centrelor de Securitate Cibernetică și Centrul de Competență pentru Inovare

[5] (Magrassi 2002a)
[6] (Magrassi 2002b)
[7] (Coats 2021)
[8] (Congressional Research Service 2020)
[9] (Tang 2020)
[10] (Smith 2019)
[11] (Congressional Research Service 2020)
[12] (Kadlecová et al. 2020)
[13] (Kadlecová et al. 2020)
[14] (Davenport și Kalakota 2019)
[15] (CS Europe 2023)

și Operațiuni (ECHO)[16] reunesc 30 de parteneri din 15 state membr, iar SPARTA[17] este formată din 44 de parteneri care implică 14 state membre.



(Tehnologia Internet of Battlefield Things într-un mediu urban nestructurat, haotic)

În 2016, U.S. Army Research Laboratory (ARL) a creat proiectul Internet of Battlefield Things (IoBT) pentru o mai bună integrare a tehnologiei IoT în operațiunile militare[18].

La 20 iulie 2017, guvernul chinez a lansat o strategie pentru a deveni lider mondial în AI până în 2030[19]. În același an, Vladimir Putin declara că „oricine devine lider în acest domeniu va conduce lumea."[20]

În 2017, ARL a înființat Internet of Battlefield Things Collaborative Research Alliance (IoBT-CRA) pentru a avansa bazele teoretice ale sistemelor IoBT[21]. {012} De

---

[16] (EMK 2023)
[17] (SPARTA 2023)
[18] (CRA 2017)
[19] (State Council 2017)
[20] (Simonite 2017)
[21] (Polit 2018)

asemenea, DARPA (SUA) a dezvoltat in program numit Ocean of Things, pentru o conștientizare a situației maritime persistente pe zone mari oceanice[22].

În 2018, guvernul german a stabilit o strategie pentru inteligența artificială, prin o colaborare cu francezii, cu sarcini în securitatea cibernetică.În Germania, inteligența artificială este abordată prin securitatea cibernetică, recunoscută ca o sarcină guvernamentală cu responsabilități împărțite în trei ministere: Ministerul Federal de Interne, Ministerul Federal al Apărării și Ministerul de Externe Federal, și mai multe instituții cu obiective specifice[23].

Strategia de Apărare Națională a SUA, lansată în ianuarie 2018, a identificat inteligența artificială drept una dintre tehnologiile cheie care „va asigura că [Statele Unite] vor fi capabile să lupte și să câștige războaiele. a viitorului."[24] Direcția Națională de Informații din SUA, a emis Inițiativa AIM în 2019[25], o strategie concepută pentru a adăuga informații cu ajutorul mașinilor, permițând serviciilor de informații să proceseze cantități uriașe de date mai rapid decât înainte și să permită ofițerilor de informații umane să se ocupă de alte sarcini. {001} Armata americană a integrat deja sisteme AI în luptă prin Projectul Maven, pentru a identifica țintele insurgenților în Irak și Siria[26]. În ultimii ani, Departamentul Apărării SUA au inițiat mai multe proiecte bazate pe IoMT și inteligența artificială, precum Connected Soldier pentru echipamente individuale inteligente[27].

În Marea Britanie strategia privind inteligența artificială are o relevanță deosebită pentru toți cei implicați în Dezvoltarea Forțelor de Apărare și Transformarea Apărării, pentru un sistem „pregătit pentru IA". S-a pus în aplicare Strategia digitală pentru apărare (2021)[28] și Strategia de date pentru apărare (2021)[29], creându-se un nou centru digital de IA. Unele elemente vor fi furnizate sau susținute de panDefence, pe baza unei not strategii IA[30].

---

[22] (MeriTalk 2018)
[23] (Kadlecová et al. 2020)
[24] (Department of Defense 2018)
[25] (AIM 2019)
[26] (Weisgerber 2017)
[27] (Stackpole 2016)
[28] (Ministry of Defence 2021b)
[29] (Ministry of Defence 2021a)
[30] (Ministry of Defence 2022)

O utilizare proeminentă a inteligenței artificiale de către Ucraina în conflictul cu Rusia este utilizarea de software de recunoaștere facială pentru a descoperi atacatorii ruși și pentru a identifica ucrainenii uciși în războiul în curs[31].Putin recunoaște puterea și oportunitățile armelor care folosesc IA, afirmând că inteligența artificială este viitorul întregii omeniri[32]. După ce Rusia a invadat Ucraina la 24 februarie 2022, armata ucraineană folosește drone[33] care pot decola, ateriza și naviga în mod autonom, și care ”pot primi informații colectate de operațiunile de supraveghere ale Statelor Unite cu privire la informațiile pe câmpul de luptă și securitatea națională despre Rusia”[34]. Rusia folosește, la rândul ei, IA pentru a analiza datele câmpului de luptă din imaginile de supraveghere.

Cursa înarmărilor cu inteligență artificială este în curs de desfășurare, în principal între marile puteri[35]. În prezent există o campanie la nivel global pentru a opri interzicerea roboților ucigași, existând o petiție[36] către Națiunile Unite prin care se solicită noi reglementări privind dezvoltarea și utilizarea tehnologiilor AI.

Concluzie

Domeniul analizei intelligence se află într-un punct de inflexiune, cu un viitor care abia se întrevede, dar modelat de efectele puternice și potențial perturbatoare ale inteligenței artificiale, megadatelor (big data) și învățării automate, asupra a ceea ce a fost mult timp un efort uman la scară intimă, adesea mai mult artă decât știință, și care depindea de informațiile individuale și de reputația analistului. Inteligența artificială și învățarea automată au devenit părți esențiale ale proceselor analitice, iar rețelele adverse generative au permis computerelor să execute rapid sarcini care în mod tradițional ar fi avut nevoie de câțiva ani pentru a se finaliza.

Bibliografie

AIM. 2019. „The AIM Initiative: A Strategy for Augmenting Intelligence Using Machines”. 2019. https://www.dni.gov/index.php/newsroom/reports-

[31] (Tegler 2022)
[32] (Gigova 2017)
[33] (BSI 2023)
[34] (Tucker 2022)
[35] (Gambrell și Isidro 2022)
[36] (Vincent 2017)

publications/reports-publications-2019/3286-the-aim-initiative-a-strategy-for-augmenting-intelligence-using-machines.

BSI. 2023. „Federal Office for Information Security". Federal Office for Information Security. 6 noiembrie 2023. https://www.bsi.bund.de/EN/Home/home_node.html.

Coats, Daniel. 2021. „Intelligence Community Information Environment (IC IE) - Data Strategy". https://www.dni.gov/files/documents/CIO/Data-Strategy_2017-2021_Final.pdf.

Congressional Research Service. 2020. „Artificial Intelligence and National Security (R45178)". 2020. https://crsreports.congress.gov/product/details?prodcode=R45178.

CRA. 2017. „Internet of Battlefield Things (IoBT) CRA – DEVCOM Army Research Laboratory". 2017. https://arl.devcom.army.mil/cras/iobt-cra/.

CS Europe. 2023. „Cyber Security Europe | Cyber Security Insight for Boardroom and C-Suite Executives." Cyber Security Europe. 2023. https://www.cseurope.info/.

Davenport, Thomas, și Ravi Kalakota. 2019. „The Potential for Artificial Intelligence in Healthcare". *Future Healthc J* 6 (2): 94–98. https://doi.org/10.7861/futurehosp.6-2-94.

Day, Peter. 2016. „Peter Day's World of Business Podcast". 2016. http://downloads.bbc.co.uk/podcasts/radio/worldbiz/worldbiz_20150319-0730a.mp3.

Department of Defense. 2018. „Summary of the 2018 National Defense Strategy". https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

EMK, SU. 2023. „ECHO Network". 2023. https://echonetwork.eu/.

Gambrell, Dorothy, și Charissa Isidro. 2022. „A Visual Guide to the World's Military Budgets". *Bloomberg.Com*, 11 martie 2022. https://www.bloomberg.com/news/features/2022-03-11/the-largest-militaries-visualized.

Gigova, Radina. 2017. „Who Putin thinks will rule the world | CNN". 2017. https://edition.cnn.com/2017/09/01/world/putin-artificial-intelligence-will-rule-world/index.html.

Kadlecová, Lucie, Nadia Meyer, Rafaël Cos, și Pauline Ravinet. 2020. „Mapping the Role of Science Diplomacy in the Cyber Field".

Lakhwani, Kamlesh, Hemant Kumar Gianey, Joseph Kofi Wireko, și Kamal Kant Hiran. 2020. *Internet of Things (IoT): Principles, Paradigms and Applications of IoT*. Place of publication not identified: BPB Publications. https://proxy.library.cornell.edu/sso/skillport?context=151247.

Magrassi, Paolo. 2002a. *Why a Universal RFID Infrastructure Would Be a Good Thing*.

———. 2002b. *A World of Smart Objects: The Role of Auto-Identification Technologies*.

MeriTalk. 2018. „DARPA Floats a Proposal for the Ocean of Things". 2018. https://www.meritalk.com/articles/darpa-floats-a-proposal-for-the-ocean-of-things/.

Ministry of Defence. 2021a. „Data Strategy for Defence". GOV.UK. 2021. https://www.gov.uk/government/publications/data-strategy-for-defence.

———. 2021b. „Digital Strategy for Defence". GOV.UK. 2021. https://www.gov.uk/government/publications/digital-strategy-for-defence-delivering-the-digital-backbone-and-unleashing-the-power-of-defences-data.

———. 2022. „Defence Artificial Intelligence Strategy". GOV.UK. 2022. https://www.gov.uk/government/publications/defence-artificial-intelligence-strategy/defence-artificial-intelligence-strategy.

Polit, Kate. 2018. „Army Takes on Wicked Problems With the Internet of Battlefield Things". 2018. https://www.meritalk.com/articles/army-takes-on-wicked-problems-with-the-internet-of-battlefield-things/.

Simonite, Tom. 2017. „Artificial Intelligence Fuels New Global Arms Race". *Wired*, 2017. https://www.wired.com/story/for-superpowers-artificial-intelligence-fuels-new-global-arms-race/.

Smith, Craig. 2019. „Eye On AI". Eye On AI. 28 august 2019. https://www.eye-on.ai.

SPARTA. 2023. „SPARTA Consortium". 2023. https://www.cybersecurityintelligence.com/sparta-consortium-5594.html.

Stackpole, Beth. 2016. „Keeping the Connected Soldier Connected with Simulation". Digital Engineering. 1 septembrie 2016. https://www.digitalengineering247.com/article/keeping-the-connected-soldier-connected-with-simulation.

State Council. 2017. „A Next Generation Artificial Intelligence Development Plan". *China Copyright and Media* (blog). 20 iulie 2017. https://chinacopyrightandmedia.wordpress.com/2017/07/20/a-next-generation-artificial-intelligence-development-plan/.

Tang, Author: Hazel. 2020. „Preparing for the Future of Artificial Intelligence. Executive Office of the President: National Science and Technology Council and Committee on Technology. October, 2016." *AIMed* (blog). 9 aprilie 2020. https://ai-med.io/executive/preparing-for-the-future-of-artificial-intelligence-executive-office-of-the-president-national-science-and-technology-council-and-committee-on-technology-october-2016/.

Tegler, Eric. 2022. „The Vulnerability of AI Systems May Explain Why Russia Isn't Using Them Extensively in Ukraine". Forbes. 2022. https://www.forbes.com/sites/erictegler/2022/03/16/the-vulnerability-of-artificial-intelligence-systems-may-explain-why-they-havent-been-used-extensively-in-ukraine/.

Townley, Dafydd. 2023. „Intelligence Agencies Have Used AI since the Cold War – but Now Face New Security Challenges". University of Portsmouth. 4 mai 2023. https://www.port.ac.uk/news-events-and-blogs/blogs/security-and-risk/intelligence-agencies-have-used-ai-since-the-cold-war-but-now-face-new-security-challenges.

Tucker, Patrick. 2022. „AI Is Already Learning from Russia's War in Ukraine, DOD Says". Defense One. 21 aprilie 2022. https://www.defenseone.com/technology/2022/04/ai-already-learning-russias-war-ukraine-dod-says/365978/.

Vincent, James. 2017. „Elon Musk and AI Leaders Call for a Ban on Killer Robots". The Verge. 21 august 2017. https://www.theverge.com/2017/8/21/16177828/killer-robots-ban-elon-musk-un-petition.

Weisgerber, Marcus. 2017. „The Pentagon's New Algorithmic Warfare Cell Gets Its First Mission: Hunt ISIS". Defense One. 14 mai 2017. https://www.defenseone.com/technology/2017/05/pentagons-new-algorithmic-warfare-cell-gets-its-first-mission-hunt-isis/137833/.